EXHIBIT C-12
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 6 ('661 Patent)	**U.S. 5,216,713 to Lindholm ("Lindholm '713")**
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:8-12 – "The present invention includes a method and apparatus for preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial image." 1:24-32 – "Raster scanned signals in display screens, laser printers, telefaxes and other computer and IT equipment contain radio frequency components, which are radiated to the surroundings and are propagated through the air and via conductors connected to the object in question, or situated close to it. The information content in these signals can be intercepted and interpreted remotely, without the user noticing anything, which is a great hazard to data security." 1:57-60 – "The object invention is to provide a method and achieve an apparatus for preventing, in a considerably more effective way, the extraneous detection of signal information in raster scan signals." 1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." Claim 1 – "Method of preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial images, characterized in that a random signal sequence is synchronized with the raster scan signals so as to have a bit frequency which is constant and equal to the bit frequency of the information-carrying raster scan signals but without information content, is generated and transmitted as protection for the raster scan signals." *See also* Scott Guthery, "Smart Cards," May 28, 1998, www.usenix.org/publications/login/1998-5/guthery.html (visited Dec. 5, 2006) ("Single-chip smart card processors based on these cores are made by almost all the large silicon foundries . . . .Several marketplace forces are at work to open the smart card as a general-purpose

	computing platform."). *See generally* U.S. Patent No. 5,944,833 to Ugon.
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:37-42 – "The generator has the task of generating a random bit sequence in time with the pixel clock. The pixel clock can be received via a separate input to the unit 3 in FIG. 1, or clocking can be generated synthetically at 2 in the FIG. The generated random bit sequence is fed to a switching element 5 via an adaption unit 4." 4:60-64 – "Separate inputs to the synchronisation equipment 3 in Figs 1 and 2 are utilised to ensure perfect synchronisation with the protected object. Inputs to the synchronisation equipment are available for.the image frequency f_b, line frequency f_j and pixel frequency f_p." Figures 1, 2.
(b) a source of unpredictable information;	1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." 2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers." 3:59-62 – "In the case where the shift register 12 is of the PISO type, according to the above, the microprocessor 10 calculates a random number with the aid of a random number algorithm."
(c) a processor:	2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to

	generate new starting conditions for the shift registers." 3:43-44 – "The generator includes a microprocessor, 10, the output data from which are fed to a shift, register 12." Figures 1, 2.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	3:37-42 – "The generator has the task of generating a random bit sequence in time with the pixel clock. The pixel clock can be received via a separate input to the unit 3 in FIG. 1, or clocking can be generated synthetically at 2 in the FIG. The generated random bit sequence is fed to a switching element 5 via an adaption unit 4." 3:59-62 – "In the case where the shift register 12 is of the PISO type, according to the above, the microprocessor 10 calculates a random number with the aid of a random number algorithm." 4:32-52 – "Another way of realising the generator in the apparatus according to the invention is to merge the output signals from an arbitrary number of programable dividers, 14, which are clocked from the pixel clock 2, see FIG. 2. The programable dividers 14 are programed from a microprocessor 10 with a plurality of integers that are randomly generated by implementing a random number algorithm in the microprocessor 10, and with which the frequency of the pixel clock 2 is divided down in the respective divider 14. When the signals (pulse trains) obtained from the different dividers 14 are merged or added in the unit 4 a resulting output signal is obtained, which can be said to represent a "grey scale" for the transmitted video signal, and when the dividers 14, during the random number generation of the microprocessor 10, perform the dividing down with precisely the instant number, there is generated a synchronised signal quantity, which varies as new numbers are entered. In this way, long random number sequences may be generated using a microprocessor having a limited rate."
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional	5:21-27 – "A certain part of the information-carrying signal will propagate on the line, e.g. a power line, when the signal radiates out, inter alia on to metallic conductors. To minimise this effect, a special filter 27 is cascade connected with the filter normally present in the computer for attenuating network noise. This is illustrated in the lower part of FIG. 3." Figure 3.

electricity in said microchip during said processing; and	
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	2:57-61 – "It is thus possible to adjust the output signal level through different frequency ranges, so that the signal level of the generated random bit frequency is equal to or higher than the level of the signal to be protected." 2:66-3:5 – "The primary winding of the current transformer carries the output signal, which generates currents on the secondary side screen, whereby the same radiated structure is utilised as for the raster scan signal, which means that the random bit sequence is emitted to the surroundings with the same radiation characteristic as the information-carrying signal." 4:41-52 – "When the signals (pulse trains) obtained from the different dividers 14 are merged or added in the unit 4 a resulting output signal is obtained, which can be said to represent a "grey scale" for the transmitted video signal, and when the dividers 14, during the random number generation of the microprocessor 10, perform the dividing down with precisely the instant number, there is generated a synchronised signal quantity, which varies as new numbers are entered. In this way, long random number sequences may be generated using a microprocessor having a limited rate."

Claim 9 ('661 Patent)	**U.S. 5,216,713 to Lindholm**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:8-12 – "The present invention includes a method and apparatus for preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial image." 1:24-32 – "Raster scanned signals in display screens, laser printers, telefaxes and other computer and IT equipment contain radio frequency components, which are radiated to the surroundings and are propagated through the air and via conductors connected to the object in question, or situated close to it. The information content in these signals can be intercepted and interpreted remotely, without the user noticing anything, which is a great hazard to data security." 1:57-60 – "The object invention is to provide a method and achieve an apparatus for preventing, in a considerably more effective way, the

	extraneous detection of signal information in raster scan signals." 1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." Claim 1 – "Method of preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial images, characterized in that a random signal sequence is synchronized with the raster scan signals so as to have a bit frequency which is constant and equal to the bit frequency of the information-carrying raster scan signals but without information content, is generated and transmitted as protection for the raster scan signals."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:37-42 – "The generator has the task of generating a random bit sequence in time with the pixel clock. The pixel clock can be received via a separate input to the unit 3 in FIG. 1, or clocking can be generated synthetically at 2 in the FIG. The generated random bit sequence is fed to a switching element 5 via an adaption unit 4." 4:60-64 – "Separate inputs to the synchronisation equipment 3 in Figs 1 and 2 are utilised to ensure perfect synchronisation with the protected object. Inputs to the synchronisation equipment are available for the image frequency f_b, line frequency f_l and pixel frequency f_p." Figures 1, 2.
(b) a source of unpredictable information;	1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." 2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to

	generate new starting conditions for the shift registers." 3:59-62 – "In the case where the shift register 12 is of the PISO type, according to the above, the microprocessor 10 calculates a random number with the aid of a random number algorithm."
(c) a processor:	2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers." 3:43-44 – "The generator includes a microprocessor, 10, the output data from which are fed to a shift, register 12." Figures 1, 2.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	3:37-42 – "The generator has the task of generating a random bit sequence in time with the pixel clock. The pixel clock can be received via a separate input to the unit 3 in FIG. 1, or clocking can be generated synthetically at 2 in the FIG. The generated random bit sequence is fed to a switching element 5 via an adaption unit 4." 3:59-62 – "In the case where the shift register 12 is of the PISO type, according to the above, the microprocessor 10 calculates a random number with the aid of a random number algorithm." 4:32-52 – "Another way of realising the generator in the apparatus according to the invention is to merge the output signals from an arbitrary number of programable dividers, 14, which are clocked from the pixel clock 2, see FIG. 2. The programable dividers 14 are programed from a microprocessor 10 with a plurality of integers that are randomly generated by implementing a random number algorithm in the microprocessor 10, and with which the frequency of the pixel clock 2 is divided down in the respective divider 14. When the signals (pulse trains) obtained from the different dividers 14 are merged or added in the unit 4 a resulting output signal is obtained, which can be said to represent a "grey scale" for the transmitted video signal, and when the dividers 14, during the random number generation of the microprocessor 10, perform the dividing down with precisely the instant number, there is generated a synchronised signal quantity, which varies as new numbers are entered. In this way, long random number sequences may be generated using a microprocessor having a

	limited rate."
(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity;	5:21-27 – "A certain part of the information-carrying signal will propagate on the line, e.g. a power line, when the signal radiates out, inter alia on to metallic conductors. To minimise this effect, a special filter 27 is cascade connected with the filter normally present in the computer for attenuating network noise. This is illustrated in the lower part of FIG. 3." 1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." Figure 3. Abstract – "In a extraneous of signal method of preventing detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial images there is generated a random signal sequence, correlated with the information-carrying raster scan signals, but without information content, which is transmitted as protection for the raster scan signals. An apparatus for this purpose includes a generator (10,12) adapted for generating a random signal sequence synchronous with the raster scan signals, and a switching element (5) adapted to transmit the random signal sequence round the equipment containing the raster scan signals that are to be protected."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof;	2:57-61 - "It is thus possible to adjust the output signal level through different frequency ranges, so that the signal level of the generated random bit frequency is equal to or higher than the level of the signal to be protected." 2:66-3:5 – "The primary winding of the current transformer carries the output signal, which generates currents on the secondary side screen, whereby the same radiated structure is utilised as for the raster scan signal, which means that the random bit sequence is emitted to the surroundings with the same radiation characteristic as the information-carrying signal." 4:41-52 – "When the signals (pulse trains) obtained from the different dividers 14 are merged or added in the unit 4 a resulting output signal is obtained, which can be said to represent a "grey scale" for the transmitted video signal, and when the dividers 14, during the random number generation of the microprocessor 10, perform the dividing

	down with precisely the instant number, there is generated a synchronised signal quantity, which varies as new numbers are entered. In this way, long random number sequences may be generated using a microprocessor having a limited rate."
(e) a hardware-implemented noise production subunit connected to said source of unpredictable information and configured to expend unpredictable amounts of electricity based on the output of said source of unpredictable information; and	2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers."
(f) an activation controller, which may be activated by software contained in said device, to activate and deactivate said expending of unpredictable amounts of electricity.	2:53-61 – "In accordance with a second advantageous embodiment of the apparatus according to the invention, an adaption unit is arranged between the generator and switching element to enable adjustment of the output signal level as a function of the frequency. It is thus possible to adjust the output signal level through different frequency ranges, so that the signal level of the generated random bit frequency is equal to or higher than the level of the signal to be protected." 5:11-18 – "In all the embodiments according to FIGS. 1 through 3 there is an adaption unit after the random bit stream generator to enable individual adjustment of the output signal level as a function of the frequency, so that the output signal level within different frequency ranges will be equal to, or higher than the level of the information-carrying signal that is to be protected. The adaption unit 4 includes, inter alia, filter links."

Claim 10 ('661 Patent)	**U.S. 5,216,713 to Lindholm**
The device of claim 9 wherein said source of unpredictable information is a hardware-implemented random number	2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a

generator, and wherein said noise production subunit includes a digital-to-analog converter.	plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers." 4:32-52 – "Another way of realising the generator in the apparatus according to the invention is to merge the output signals from an arbitrary number of programable dividers, 14, which are clocked from the pixel clock 2, see FIG. 2. The programable dividers 14 are programed from a microprocessor 10 with a plurality of integers that are randomly generated by implementing a random number algorithm in the microprocessor 10, and with which the frequency of the pixel clock 2 is divided down in the respective divider 14. When the signals (pulse trains) obtained from the different dividers 14 are merged or added in the unit 4 a resulting output signal is obtained, which can be said to represent a "grey scale" for the transmitted video signal, and when the dividers 14, during the random number generation of the microprocessor 10, perform the dividing down with precisely the instant number, there is generated a synchronised signal quantity, which varies as new numbers are entered. In this way, long random number sequences may be generated using a microprocessor having a limited rate." *See also, e.g.*, English abstracts of JP10084223, JP10197610, JP62260406, and JP62082702 (describing including a digital to analog converter in a noise production subunit).

Claim 11 ('661 Patent)	**U.S. 5,216,713 to Lindholm**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	1:8-12 – "The present invention includes a method and apparatus for preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial image." 1:24-32 – "Raster scanned signals in display screens, laser printers, telefaxes and other computer and IT equipment contain radio frequency components, which are radiated to the surroundings and are propagated through the air and via conductors connected to the object in question, or situated close to it. The information content in these signals can be intercepted and interpreted remotely, without the user noticing anything, which is a great hazard to data security." 1:57-60 – "The object invention is to provide a method and achieve an apparatus for preventing, in a considerably more effective way, the

	extraneous detection of signal information in raster scan signals." 1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." Claim 1 – "Method of preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial images, characterized in that a random signal sequence is synchronized with the raster scan signals so as to have a bit frequency which is constant and equal to the bit frequency of the information-carrying raster scan signals but without information content, is generated and transmitted as protection for the raster scan signals."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:37-42 – "The generator has the task of generating a random bit sequence in time with the pixel clock. The pixel clock can be received via a separate input to the unit 3 in FIG. 1, or clocking can be generated synthetically at 2 in the FIG. The generated random bit sequence is fed to a switching element 5 via an adaption unit 4." 4:60-64 – "Separate inputs to the synchronisation equipment 3 in Figs 1 and 2 are utilised to ensure perfect synchronisation with the protected object. Inputs to the synchronisation equipment are available for the image frequency f_b, line frequency f_l and pixel frequency f_p." Figures 1, 2.
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	3:37-42 – "The generator has the task of generating a random bit sequence in time with the pixel clock. The pixel clock can be received via a separate input to the unit 3 in FIG. 1, or clocking can be generated synthetically at 2 in the FIG. The generated random bit sequence is fed to a switching element 5 via an adaption unit 4." 4:60-64 – "Separate inputs to the synchronisation equipment 3 in Figs 1 and 2 are utilised to ensure perfect synchronisation with the protected object. Inputs to the synchronisation equipment are available for the image frequency f_b, line frequency f_l and pixel frequency f_p."
(c) a processor connected to said input interface for	2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal

receiving and cryptographically processing said quantity; and	sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers." 3:43-44 – "The generator includes a microprocessor, 10, the output data from which are fed to a shift, register 12." Figures 1, 2.
(d) a noise production system for introducing noise into said measurement of said power consumption.	1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." 2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers." 3:59-62 – "In the case where the shift register 12 is of the PISO type, according to the above, the microprocessor 10 calculates a random number with the aid of a random number algorithm."

Claim 12 ('661 Patent)	**U.S. 5,216,713 to Lindholm**
The device of claim 11 wherein said noise production system comprises: (a) a source of randomness for generating initial noise having a random characteristic;	1:65-2:12 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation. According to a first advantageous embodiment of the method according to the invention the starting condition for the random signal sequence of output data is determined by calculation of a so-called

	chaos algorithm, according to the principles given by Alan Rodney Murch, 'Technological Applications of Deterministic Chaos', University of Canterbury, Christchurch, New Zealand, July, 1989."
(b) a noise processing module for improving the random characteristic of said initial noise; and	1:65-2:12 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation. According to a first advantageous embodiment of the method according to the invention the starting condition for the random signal sequence of output data is determined by calculation of a so-called chaos algorithm, according to the principles given by Alan Rodney Murch, 'Technological Applications of Deterministic Chaos', University of Canterbury, Christchurch, New Zealand, July, 1989." 2:53-61 – "In accordance with a second advantageous embodiment of the apparatus according to the invention, an adaption unit is arranged between the generator and switching element to enable adjustment of the output signal level as a function of the frequency. It is thus possible to adjust the output signal level through different frequency ranges, so that the signal level of the generated random bit frequency is equal to or higher than the level of the signal to be protected."
(c) a noise production module configured to vary said power consumption based on an output of said noise processing module.	1:65-2:12 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation. According to a first advantageous embodiment of the method according to the invention the starting condition for the random signal sequence of output data is determined by calculation of a so-called chaos algorithm, according to the principles given by Alan Rodney Murch, 'Technological Applications of Deterministic Chaos', University of Canterbury, Christchurch, New Zealand, July, 1989." 2:53-61 – "In accordance with a second advantageous embodiment of the apparatus according to the invention, an adaption unit is arranged between the generator and switching element to enable adjustment of the output signal level as a function of the frequency. It is thus possible to adjust the output signal level through different frequency ranges, so that the signal level of the generated random bit frequency is equal to or higher than the level of the signal to be protected."

Claim 13 ('661 Patent)	U.S. 5,216,713 to Lindholm
The device of claim 12 wherein said noise production system is connected to said processor and is selectively operable under the control of said processor.	2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers."

Claim 27 ('661 Patent)	U.S. 5,216,713 to Lindholm
A method of securely performing a cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	1:8-12 – "The present invention includes a method and apparatus for preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial image." 1:24-32 – "Raster scanned signals in display screens, laser printers, telefaxes and other computer and IT equipment contain radio frequency components, which are radiated to the surroundings and are propagated through the air and via conductors connected to the object in question, or situated close to it. The information content in these signals can be intercepted and interpreted remotely, without the user noticing anything, which is a great hazard to data security." 1:57-60 – "The object invention is to provide a method and achieve an apparatus for preventing, in a considerably more effective way, the extraneous detection of signal information in raster scan signals." 1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." 1:65-2:12 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation.

	According to a first advantageous embodiment of the method according to the invention the starting condition for the random signal sequence of output data is determined by calculation of a so-called chaos algorithm, according to the principles given by Alan Rodney Murch, 'Technological Applications of Deterministic Chaos', University of Canterbury, Christchurch, New Zealand, July, 1989." Claim 1 – "Method of preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial images, characterized in that a random signal sequence is synchronized with the raster scan signals so as to have a bit frequency which is constant and equal to the bit frequency of the information-carrying raster scan signals but without information content, is generated and transmitted as protection for the raster scan signals."
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:37-42 – "The generator has the task of generating a random bit sequence in time with the pixel clock. The pixel clock can be received via a separate input to the unit 3 in FIG. 1, or clocking can be generated synthetically at 2 in the FIG. The generated random bit sequence is fed to a switching element 5 via an adaption unit 4." 4:60-64 – "Separate inputs to the synchronisation equipment 3 in Figs 1 and 2 are utilised to ensure perfect synchronisation with the protected object. Inputs to the synchronisation equipment are available for the image frequency f_b, line frequency f_l and pixel frequency f_p." Figures 1, 2.
(b) generating unpredictable information;	1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." 2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers."

	3:59-62 – "In the case where the shift register 12 is of the PISO type, according to the above, the microprocessor 10 calculates a random number with the aid of a random number algorithm."
(c) using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by using said unpredictable information to modify said sequence; and	5:21-27 – "A certain part of the information-carrying signal will propagate on the line, e.g. a power line, when the signal radiates out, inter alia on to metallic conductors. To minimise this effect, a special filter 27 is cascade connected with the filter normally present in the computer for attenuating network noise. This is illustrated in the lower part of FIG. 3." Figure 3.
(d) outputting said cryptographically processed quantity to a recipient thereof.	2:57-61 – "It is thus possible to adjust the output signal level through different frequency ranges, so that the signal level of the generated random bit frequency is equal to or higher than the level of the signal to be protected." 2:66-3:5 – "The primary winding of the current transformer carries the output signal, which generates currents on the secondary side screen, whereby the same radiated structure is utilised as for the raster scan signal, which means that the random bit sequence is emitted to the surroundings with the same radiation characteristic as the information-carrying signal." 4:41-52 – "When the signals (pulse trains) obtained from the different dividers 14 are merged or added in the unit 4 a resulting output signal is obtained, which can be said to represent a "grey scale" for the transmitted video signal, and when the dividers 14, during the random number generation of the microprocessor 10, perform the dividing down with precisely the instant number, there is generated a synchronised signal quantity, which varies as new numbers are entered. In this way, long random number sequences may be generated using a microprocessor having a limited rate."

Claim 29 ('661 Patent)	**U.S. 5,216,713 to Lindholm**
A method of securely performing a cryptographic processing	1:8-12 – "The present invention includes a method and apparatus for preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an

operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	image or partial image." 1:24-32 – "Raster scanned signals in display screens, laser printers, telefaxes and other computer and IT equipment contain radio frequency components, which are radiated to the surroundings and are propagated through the air and via conductors connected to the object in question, or situated close to it. The information content in these signals can be intercepted and interpreted remotely, without the user noticing anything, which is a great hazard to data security." 1:57-60 – "The object invention is to provide a method and achieve an apparatus for preventing, in a considerably more effective way, the extraneous detection of signal information in raster scan signals." 1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." Claim 1 – "Method of preventing extraneous detection of signal information from raster scan signals in a plurality of consecutive line signals intended to form an image or partial images, characterized in that a random signal sequence is synchronized with the raster scan signals so as to have a bit frequency which is constant and equal to the bit frequency of the information-carrying raster scan signals but without information content, is generated and transmitted as protection for the raster scan signals."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	3:37-42 – "The generator has the task of generating a random bit sequence in time with the pixel clock. The pixel clock can be received via a separate input to the unit 3 in FIG. 1, or clocking can be generated synthetically at 2 in the FIG. The generated random bit sequence is fed to a switching element 5 via an adaption unit 4." 4:60-64 – "Separate inputs to the synchronisation equipment 3 in Figs 1 and 2 are utilised to ensure perfect synchronisation with the protected object. Inputs to the synchronisation equipment are available for the image frequency f_b, line frequency f_l and pixel frequency f_p." Figures 1, 2.
(b) receiving a quantity to be cryptographically processed, said quantity being representative of	3:37-42 – "The generator has the task of generating a random bit sequence in time with the pixel clock. The pixel clock can be received via a separate input to the unit 3 in FIG. 1, or clocking can be generated synthetically at 2 in the FIG. The generated random bit

at least a portion of a message;	sequence is fed to a switching element 5 via an adaption unit 4." 4:60-64 – "Separate inputs to the synchronisation equipment 3 in Figs 1 and 2 are utilised to ensure perfect synchronisation with the protected object. Inputs to the synchronisation equipment are available for the image frequency f_b, line frequency f_l and pixel frequency f_p." Figures 1, 2.
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." 2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers." 3:59-62 – "In the case where the shift register 12 is of the PISO type, according to the above, the microprocessor 10 calculates a random number with the aid of a random number algorithm."
(d) outputting said cryptographically processed quantity to a recipient thereof.	2:57-61 – "It is thus possible to adjust the output signal level through different frequency ranges, so that the signal level of the generated random bit frequency is equal to or higher than the level of the signal to be protected." 2:66-3:5 – "The primary winding of the current transformer carries the output signal, which generates currents on the secondary side screen, whereby the same radiated structure is utilised as for the raster scan signal, which means that the random bit sequence is emitted to the surroundings with the same radiation characteristic as the information-carrying signal." 4:41-52 – "When the signals (pulse trains) obtained from the different dividers 14 are merged or added in the unit 4 a resulting output signal is obtained, which can be said to represent a 'grey scale' for the transmitted video signal, and when the dividers 14, during the random number generation of the microprocessor 10, perform the dividing

	down with precisely the instant number, there is generated a synchronised signal quantity, which varies as new numbers are entered. In this way, long random number sequences may be generated using a microprocessor having a limited rate."

Claim 30 ('661 Patent)	**U.S. 5,216,713 to Lindholm**
The method of claim 29 wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic;	1:65-2:4 – "With the present invention there is thus generated a random signal sequence perfectly correlated to the raster scanned information-carrying signals which is transmitted as protection for the raster scanned signals. While uncorrelated signals may be comparatively easily filtered off, correlated signals are difficult to filter and accordingly can not be filtered by mean value formation." 2:42-52 – "In accordance with a first advantageous embodiment, sparing of components, of the apparatus according to the invention, the apparatus comprises a generator for producing the random signal sequence, which generator includes a microprocessor and a shift register of so-called maximum length feedback kind, which shift register is made up from individual feedback shift registers of a plurality such that the repetition cycle exceeds the time for generating the number of pixels per image, said microprocessor being adapted to generate new starting conditions for the shift registers."
(b) improving the random characteristic of said initial noise; and	2:53-61 – "In accordance with a second advantageous embodiment of the apparatus according to the invention, an adaption unit is arranged between the generator and switching element to enable adjustment of the output signal level as a function of the frequency. It is thus possible to adjust the output signal level through different frequency ranges, so that the signal level of the generated random bit frequency is equal to or higher than the level of the signal to be protected." 5:11-18 – "In all the embodiments according to FIGS. 1 through 3 there is an adaption unit after the random bit stream generator to enable individual adjustment of the output signal level as a function of the frequency, so that the output signal level within different frequency ranges will be equal to, or higher than the level of the information-carrying signal that is to be protected."
(c) varying said power consumption based on said improved initial noise.	2:53-61 – "In accordance with a second advantageous embodiment of the apparatus according to the invention, an adaption unit is arranged between the generator and switching element to enable adjustment of the output signal level as a function of the frequency. It is thus possible to adjust the output signal level through different frequency

	ranges, so that the signal level of the generated random bit frequency is equal to or higher than the level of the signal to be protected." 5:11-18 – "In all the embodiments according to FIGS. 1 through 3 there is an adaption unit after the random bit stream generator to enable individual adjustment of the output signal level as a function of the frequency, so that the output signal level within different frequency ranges will be equal to, or higher than the level of the information-carrying signal that is to be protected."